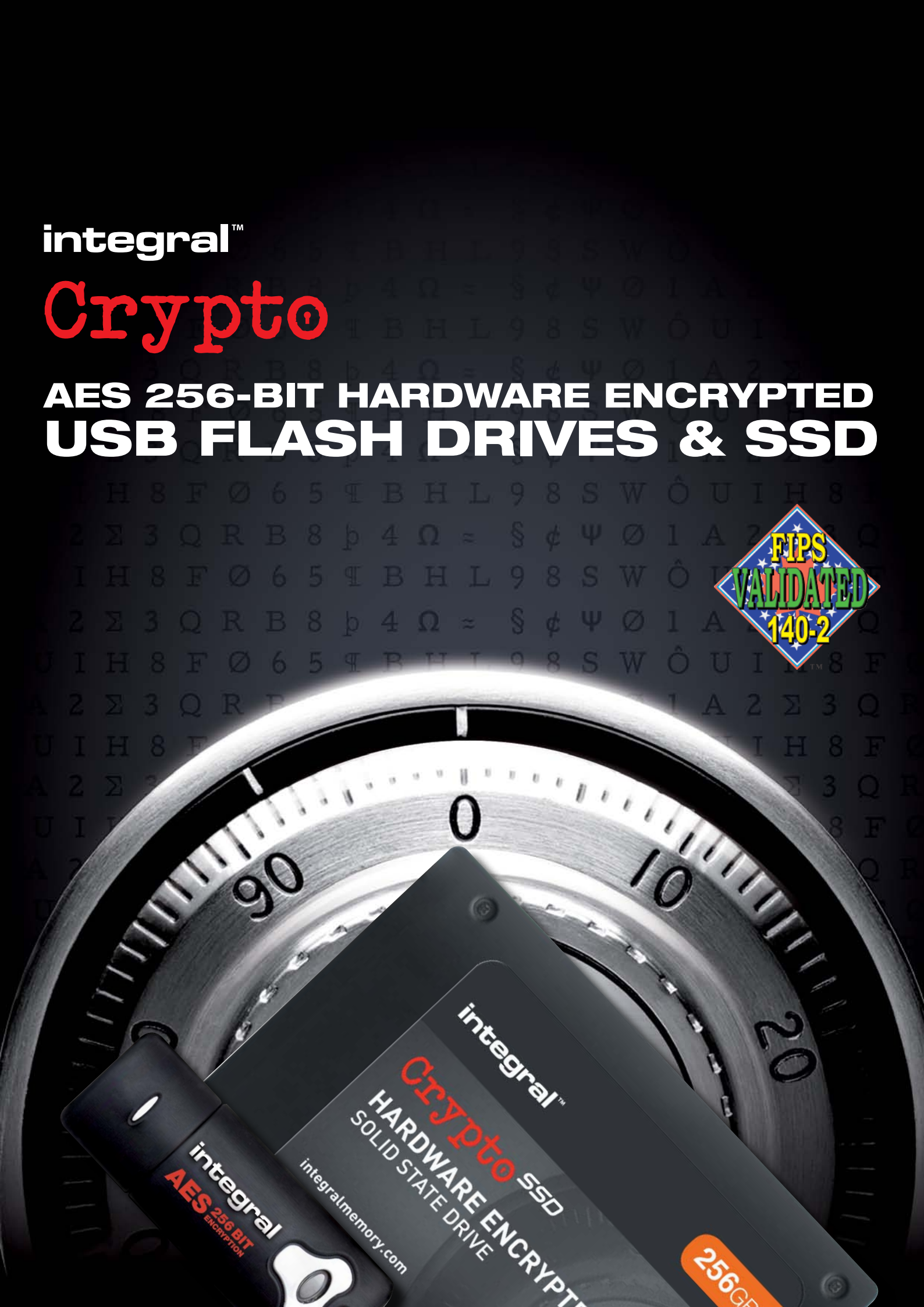
integral™

Crypto

AES 256-BIT HARDWARE ENCRYPTED USB FLASH DRIVES & SSD



About Integral Memory plc

Integral Memory was established in 1989 and has been involved in the flash storage industry since its inception. Design, R&D and testing are carried out at our HQ in London, England. We partner with Samsung, Toshiba and Intel, the industry leaders in flash technology, to bring cost effective flash memory solutions to the worldwide market.

To find out more please visit www.integralmemory.com

SEE INTEGRAL ENCRYPTED DRIVES IN ACTION!

Visit youtube.com/integralmemorytv

Crypto Drive range - User Features

AES 256-bit Hardware Encryption

AES 256-bit hardware encryption provides superior security over software encryption. Password comparisons are securely processed on the Crypto hardware.

Mandatory Encryption

All files transferred to the drive are encrypted. A user cannot save unprotected files.

Secure Entry

Encrypted data cannot be accessed without the correct high-strength 8-16 character alphanumeric password. An optional password hint can be set-up which cannot be the same as the password. Before use a high-strength password must be set.

Password Entry Count

The Crypto Drive records the failed entry count. e.g. if the Crypto is removed after 2 failed attempts and reinserted, the drive will resume with the 3rd attempt.

Brute-Force Password Attack Protection

Encrypted data is automatically erased after 6 failed password attempts. The data and encryption key are securely destroyed and the Crypto Drive is reset and can be reused.

Auto Lock

The Crypto drive will automatically encrypt all data and lock; when the drive is removed from the PC, when the screen-saver or "computer lock" function is activated.

Additionally for the Crypto Dual and Dual+ the drive will lock if left idle for more than 10 minutes.

Integral Crypto AES 256-bit hardware encrypted USB Drives

USB Flash Drive security is a challenge facing all IT departments and with many governments starting to impose hefty fines, encryption of sensitive data on USB drives is becoming compulsory.

Integral produce a range of AES 256-bit hardware encrypted USB Flash Drives that provide an easy to use, cost effective and highly secure solution that is designed to work with your end-point security.

Our Crypto Drive USB range is FIPS and CESG validated and all models have a zero footprint, so no software installation is required. All files transferred to the drive are automatically encrypted and are protected by a mandatory high-strength password. If the Crypto USB is ever lost or stolen, the drive will securely destroy all data after six failed password attempts. Crypto Drives are used and trusted worldwide by government departments, global corporations and SMEs.

The Integral Crypto DUAL and DUAL+ offer an optional master password override, in addition to a high-strength user password. If a user forgets their password the Crypto DUAL and DUAL+ drives can be accessed with a master password by an IT administrator. Crypto DUAL is also compatible with both Windows® and Mac® operating systems. Crypto DUAL+ includes the same features as the Crypto DUAL but in an expanded design, to allow for greater storage capacity, starting at 64GB and 128GB.

See the Integral Crypto Encrypted USB Drives at

integralmemory.com/crypto

Dual Password

An administrator can set up an optional master password on a drive. A user then sets a user password as normal. A warning is given to the user after the fifth failed password attempt to take the drive to the administrator to unlock the drive by using the master password. The user and master password cannot be the same.

Available on Crypto Dual and Crypto Dual+.

Rugged triple-layer waterproof design

Protects the Crypto Drive against knocks, drops, break-in and submerging in water. The electronics are sealed in epoxy resin and then shielded by a steel inner case. The rubberised silicone outer casing provides a final layer of protection.

Up to 4 ft. water; conforms to IEC 60529 IPX8.

Multilingual interface

Simple multilingual interface for “out of the box” use with minimal support; ideal for global corporations.

Zero Footprint

Crypto Drive has a zero footprint - No software installation is required before use.

Personal ID Function

As an option, contact details can be added to the Crypto that can be viewed without compromising encrypted data.

Serial Number

The USB pin on each drive is etched with a unique 7-digit code. This allows a record to be kept of which drive has been allocated to a specific user.

OS Compatibility

The Integral Crypto is available in separate PC and Mac editions.

The Integral Crypto Dual and Dual+ are compatible with PCs and Macs

(Windows XP/Vista/7 & Mac OS X).

User Manual

User manual stored on drive.

FIPS 140-2 Level 2 Validated - Cert No: 1424 FIPS 197 Cert No: 1137

Independently and stringently tested for data encryption and protection to the Federal Information Processing Standards (FIPS) managed by NIST (National Institute of Standards and Technology).

CESG Claims Tested Mark (CCTM) - Cert No: 2011 05 0097

Crypto Drives have been awarded the CESG Claims Tested Mark (CCTM) by CESG, the UK Government’s National Technical Authority for Information Assurance. Public sector buying confidence is assured.

Unique ID (Optional)

Crypto Drives can be personalised with a designated company identifying name or number. This will allow a Network Administrator to block access to unrecognised USBs for security purposes, whilst allowing the Integral encrypted Flash Drive to function as the ‘official’ company drive.

Customisation (Optional)

Customisation Available - Your own serial number etching, Flash Drive and GUI can be customised to suit your brand (subject to minimum order quantities).

Integral Encrypted USB Product Range

AES 256 BIT ENCRYPTION

	Crypto 140-2	Crypto 140-2 Mac Edition	Crypto 197	Crypto 197 Mac Edition	Crypto Dual 197	Crypto Dual+ 197	Crypto Dual 140-2	Crypto Dual+ 140-2
Specs								
Available Capacities	2GB, 4GB, 8GB, 16GB, 32GB	2GB, 4GB, 8GB, 16GB, 32GB	2GB, 4GB, 8GB, 16GB, 32GB	2GB, 4GB, 8GB, 16GB, 32GB	2GB, 4GB, 8GB, 16GB, 32GB	64GB, 128GB	2GB, 4GB, 8GB, 16GB, 32GB	64GB, 128GB
AES 256-bit hardware encryption	✔	✔	✔	✔	✔	✔	✔	✔
FIPS Validation	140-2 Level 2	140-2 Level 2	197	197	197	197	140-2 Level 2	140-2 Level 2
CESG Claims Tested Mark (CCTM)	✔	✔	✔	✔	-	-	-	-
Mandatory encryption of all files	✔	✔	✔	✔	✔	✔	✔	✔
Zero Footprint - No software required	✔	✔	✔	✔	✔	✔	✔	✔
Compatible with Endpoint security software	✔	✔	✔	✔	✔	✔	✔	✔
Works on Windows without administrator privileges	✔	-	✔	-	✔	✔	✔	✔
Works on Mac OS X without administrator privileges	-	✔	-	✔	✔	✔	✔	✔
Secure Entry - Password Mandatory	✔	✔	✔	✔	✔	✔	✔	✔
High-Strength Password Enforcement	✔	✔	✔	✔	✔	✔	✔	✔
Brute-Force Password Attack Protection	✔	✔	✔	✔	✔	✔	✔	✔
Auto-Lock	✔	✔	✔	✔	Locks if PC is idle for more than 10 mins	Locks if PC is idle for more than 10 mins	Locks if PC is idle for more than 10 mins	Locks if PC is idle for more than 10 mins
Password Entry Count	✔	✔	✔	✔	✔	✔	✔	✔
Personal ID Function	✔	✔	✔	✔	✔	✔	✔	✔
Rugged triple-layer waterproof design	✔	✔	✔	✔	✔	✔	✔	✔
User manual stored on drive	✔	✔	✔	✔	✔	✔	✔	✔
Multi-lingual interface	24 Languages	6 Languages	24 Languages	6 Languages	26 Languages	26 Languages	26 Languages	26 Languages
Dual Password	-	-	-	-	✔	✔	✔	✔
Dual OS - PC & Mac compatible	-	-	-	-	✔	✔	✔	✔
4 Channel access (faster read & write speeds)	-	-	-	-	-	✔	-	✔
Serial Number Etching	✔	✔	Available on request	Available on request	✔	✔	✔	✔

Capacity	Part Code	Capacity	Part Code	Capacity	Part Code	Capacity	Part Code	Capacity	Part Code	Capacity	Part Code	Capacity	Part Code	Capacity	Part Code
2GB	INFD2GCRYPTO140-2	2GB	INFD2GCRYPTOMC140-2	2GB	INFD2GCRYPTO197	2GB	INFD2GCRYPTOMAC197	2GB	INFD2GCRYPTODL197	64GB	INFD64GCRYDLPL197	2GB	INFD2GCRYPTODL140-2	64GB	INFD64GCRYDLPL140-2
4GB	INFD4GCRYPTO140-2	4GB	INFD4GCRYPTOMC140-2	4GB	INFD4GCRYPTO197	4GB	INFD4GCRYPTOMAC197	4GB	INFD4GCRYPTODL197	128GB	INFD128GCRYDLPL197	4GB	INFD4GCRYPTODL140-2	128GB	INFD128GCRYDLPL140-2
8GB	INFD8GCRYPTO140-2	8GB	INFD8GCRYPTOMC140-2	8GB	INFD8GCRYPTO197	8GB	INFD8GCRYPTOMAC197	8GB	INFD8GCRYPTODL197			8GB	INFD8GCRYPTODL140-2		
16GB	INFD16GCRYPTO140-2	16GB	INFD16GCRYPTOMC140-2	16GB	INFD16GCRYPTO197	16GB	INFD16GCRYPTOMAC197	16GB	INFD16GCRYPTODL197			16GB	INFD16GCRYPTODL140-2		
32GB	INFD32GCRYPTO140-2	32GB	INFD32GCRYPTOMC140-2	32GB	INFD32GCRYPTO197	32GB	INFD32GCRYPTOMAC197	32GB	INFD32GCRYPTODL197			32GB	INFD32GCRYPTODL140-2		

www.integralmemory.com

Protect your data with an encrypted Integral Crypto SSD

The Integral Crypto SSD is the ideal solution for data protection. When the system is shut down, 256-bit full disk encryption is instigated.

If a PC or laptop with an Integral Crypto SSD installed is lost or stolen, sensitive data is secure and cannot be accessed without the high-strength password.

Crypto SSD is the no-fuss and highly-secure solid state encryption solution for many industries including; finance, legal, health, education and government.

A direct replacement for a laptop's Hard Drive/SSD. Fits easily into any desktop PC using a fitting kit*.

*Supplied separately

Product Features

- Full 256-bit AES Hardware Encryption
- Dual password – User and Administrator override
- Hardware tied to computer when encryption is set
- Brute-force attack protection
- Anti-cloning when encryption is set
- Offers better protection then software encryption, as the data is hardware encrypted on the SSD drive
- No performance degradation when encryption is activated (compared to conventional SSD)
- High-speed sustained data transfer. Read and Write times up to 240MB/s
- No moving parts, greater resistance to shock and vibration
- Noise free, no spin or seek time
- Cuts boot time in half
- Weighs less than conventional HDD
- Uses 1/10 of the power of a normal spinning disk HDD
- Extends laptop battery life
- Super low power consumption during operation and sleep modes

GREEN COMPUTING

Technical Features

- MLC-NAND Flash Technology
- SATA II 2.5”
- SATA Revision 2.6 compliant
- TRIM option
- S.M.A.R.T. option
- Power management supported
- 128MB DDR Cache Buffer
- CE and FCC certified and RoHs compliant
- Compatible with XP, Vista and 7

Specifications

PERFORMANCE & INTERFACE	
Read	240MB/s (max)
Write	220MB/s (max)
Interface	SATA II (SATA 1.5Gbps and 3Gbps)
RELIABILITY	
Wear levelling	Static & Dynamic
MTBF	1,000,000 hours
ECC	48/32/28 bit per 2KB
Data Retention	10 years
POWER CONSUMPTION	
Power requirement	5V
Read Mode	1.4W*
Write Mode	4.7W*
Sleep Mode	0.2W
*This data is measured by Fluke 287 multimeter and the capacity is 128GB with 16 chips	
ENVIRONMENTAL	
Operating Temp	0° - +70°C
Non - Operating Temp	-40° - +85°C
Humidity	RH=95% under 55°C
Vibration	20G (80-2000Hz)
Shock	1,500G (0.5msec)
PHYSICAL	
Length	100.1mm
Width	69.9mm
Height	9.3mm
Weight	76(g)
WARRANTY	
2 Years	

Crypto SSD - User Features

AES 256-bit Hardware Encryption

AES 256-bit hardware encryption provides superior security over software encryption. Password comparisons are securely processed on the Crypto SSD.

Total Drive Encryption

All data stored on the Crypto SSD is encrypted (including the Operating System).

Secure Entry

Encrypted data cannot be accessed without the correct high-strength 8-16 character alphanumeric password. An optional password hint can be set-up which cannot be the same as the password. Before use a high-strength password must be set.

Dual Password

As an option an Administrator can setup a user password and a master override password. If the user forgets their password, the Crypto SSD can be unlocked by the Administrator and the user password reset.

Rugged Design

The electronics are sealed in tamper-free epoxy resin and then shielded by a steel outer case.

Brute-Force Password Attack Protection

Encrypted data is automatically erased after the default 6 failed password attempts (password attempts configurable to a maximum of 20). The data and encryption key are securely destroyed and the Crypto SSD is reset and can then be reused.

FIPS 197 Certified

Independently and stringently tested for data encryption and protection to the Federal Information Processing Standards (FIPS) managed by NIST (National Institute of Standards and Technology).

High-speed Read/Write

The Crypto SSD has both high encryption and the main benefit of a standard SSD; a high-speed sustained data transfer rate. Read and Write times are up to 240MB/s.

Quick boot

Using a Crypto SSD in place of a traditional HDD can cut your desktop computer or laptop's boot time in half.

Multilingual interface

Simple multilingual interface for "out of the box" use with minimal support; ideal for global corporations.

Product Ordering Information

CAPACITY	PRODUCT	PART NUMBER
32GB	Crypto SSD	INSSD32GS25MCRYPTO
64GB	Crypto SSD	INSSD64GS25MCRYPTO
128GB	Crypto SSD	INSSD128GS25MCRYPTO
256GB	Crypto SSD	INSSD256GS25MCRYPTO

1GB = 1,000,000,000 bytes. Formatted capacity is less.

Custom ID and pre-loaded content are available on request.